Virginia's Governmental Information Security

A Guide for Commonwealth Executives after September 11, 2001

Edited by Samuel T. Redwine, Jr.

June 2002

Commonwealth Information Security Center Technical Report CISC-TR-2002-002

Commonwealth Information Security Center
MSC 4103
James Madison University
Harrisonburg, Virginia 22807

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6/1/2002	Report 6/1/2002

4. TITLE AND SUBTITLE
Virginia's Governmental Information Security: A Guide for Commonwealth Executives after September 11, 2002 (CISC-TR-2002-002)

5. FUNDING NUMBERS

6. AUTHOR(S)
Redwine Jr, Samuel T.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Commonwealth Information
Security Center
MSC4103, James Madison
University, Harrisonburg, VA
22807

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The events of September 11, 2001, highlighted an increased need for information technology (IT) security not only for business and federal executives, but for state governmental executives as well. This increased urgency and heightened awareness left many of Virginia’s government executives asking the question, “How secure and prepared is the Commonwealth to deal with information security attacks?”
This report provides a brief overview of the Commonwealth’s security situation and offers executives and managers low budget actions that can be taken to begin addressing the added responsibility created by these threats, with a specific emphasis on electronic attacks. The purpose of this paper is to help the leaders in the Commonwealth understand the security posture of their organization so they can effectively suggest improvements where necessary.

14. SUBJECT TERMS
IATAC Collection, information security, government, electronic attacks, cybersecurity, physical security

15. NUMBER OF PAGES
20

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Commonwealth Information Security Center Technical Report
Series Editor: *Samuel T. Redwine, Jr.*
This Commonwealth Information Security Center Technical Report CISC-TR-2002-002 (Version 0.0.25) is a joint effort of the:

Commonwealth Information Security Center
MSC 4103
James Madison University
Harrisonburg, Virginia 22807

540.568.7389

www.cisc.jmu.edu

Department of Information Technology
Security Division
110 South 7th Street
Richmond, Virginia 23219

804.371.5000

www.dit.state.va.us

In part, a grant from the Virginia (USA) Commonwealth Technology Research Fund supported this work.

Acknowledgements

The following individuals and organizations contributed to the writing of this report:

Samuel E. Redwine, Jr.
Commonwealth Information Security Center

James E. Adams
Department of Information Technology

Randy Marchany
Virginia Polytechnic Institute and University

Cindy Allen
Commonwealth Information Security Center

Leslie Lauziere
Office of the Attorney General

Don Kendrick
Department of Motor Vehicles

Sara Gerhardt
Commonwealth Information Security Center

Allan Berg
Commonwealth Information Security Center

Shelly McCabe
Department of Information Technology

Mauri Shaw
Department of Information Technology

Fairfax County Department of Information Technology

Table of Contents

Introduction

Purpose and Scope

The events of September 11, 2001, highlighted an increased need for information technology (IT) security not only for business and federal executives, but for state governmental executives as well. This increased urgency and heightened awareness left many of Virginia's government executives asking the question, "How secure and prepared is the Commonwealth to deal with information security attacks?"

This report provides a brief overview of the Commonwealth's security situation and offers executives and managers low budget actions that can be taken to begin addressing the added responsibility created by these threats, with a specific emphasis on electronic attacks. The purpose of this paper is to help the leaders in the Commonwealth understand the security posture of their organization so they can effectively suggest improvements where necessary.

Organization of Document

This document first describes the general computer and network security problems facing IT security in the Virginia government before September 11, 2001. Next, the situation after September 11 is discussed. Finally, some low budget actions an executive or top manager might take, as well as suggestions for an initial self-assessment and for a state standard follow.

The Problem

Security Threats to Virginia's Information Technology

Background

Virginia's IT infrastructure faces multiple threats to organizational information systems, as well as having to address the special challenges faced by state agencies, local governments and higher education due to their unique missions. Today cyberspace is a quite threatening environment, presenting many potential attackers and vulnerabilities. These vulnerabilities are not limited to the private sector, but exist in the public sector as well.

Cyber Attacks in Virginia

A look at just a few of the attacks experienced by Virginia state and local government entities can give some feel for the variety of threats faced.

Universities

Both Virginia Tech and George Mason University computer security problems have made the newspapers, including the Richmond Times Dispatch and the Washington Post. One attack exploited Virginia Tech's facilities by placing pornographic material there and redirecting traffic for the New York Yankee website to the graphic located at Virginia Tech. Virginia Tech was a victim of the same attack, although press reports gave the impression that the university was involved in its commission. The compromised system was confiscated by law enforcement, resulting in the shutdown of a research laboratory for a period of time.

As a result, Virginia Tech is an example of a state organization that has devoted significant effort to computer security, including policies, risk analysis, and business impact analysis procedures; installation of software; education and training for in-house and outside IT staff; and creation of a Computer Incident Response Team (CIRT). Virginia Tech also coordinates the information flow of the higher education CIRTs in the state.

Executive Agencies

In February 2000, the Virginia Department of Motor Vehicles (DMV) experienced a cyber attack against the agency's network. The attack began at 2:00 a.m. on a Sunday morning. The agency staff was notified by the agency's Intrusion Detection System (IDS) and took counter measures to stop the attack and collect data to identify the hacker for prosecution. After taking these steps, DMV and State Virginia Police investigators gathered the proper court documents and proceeded to apprehend the suspect. The security procedures and monitoring in place led to the suspect being arrested by 4:00 a.m. Monday.

Local Government

In the fall of 2001, Fairfax County was attacked by the NIMDA computer virus. The attack began on a Tuesday evening and efforts were made to disinfect affected servers. The next day there was another infection. Representatives from all the agencies in the county met at a command center established to deal with the attack. This was necessary since Fairfax does not have a centrally managed IT system, and a centralized approach was needed to address the problem. These agency representatives worked with security consultants to devise and document a strategy that divided the network into segments and progressively cleaned them. Once all the segments were verified as virus-free, they were reactivated. In total, the virus hit on a Tuesday and by the following Tuesday all systems were virus-free and functional. Fortunately, the same lack of centralization that posed some difficulties also meant that at no time was the entire network non-operational.

Fairfax learned some valuable lessons from this experience. They have now installed a more robust anti-virus system to provide preemptive protection to their network and have begun a review of their architecture and policies and procedures. They have also begun to centrally manage and distribute software.

Community Colleges

Disgruntled employees and former employees account for a large number of the security breaches that occur to networks. In 2001, 49 percent of the respondents to the Center for Internet Security (CIS) and Federal Bureau of Investigation (FBI) survey reported unauthorized access by insiders. In no way has Virginia been sheltered from this phenomenon. In May of 2001, a former employee of Tidewater Community College was arrested and pleaded guilty in federal court for hacking into the networks of the Virginia Community College System and the University of Florida over a two-year period. The intrusions periodically blocked student access to the Internet, and the Virginia Community College System spent more than $6,000 repairing the damage and hiring outside support to assess the problem.

The above examples range across state and local government, universities, attacks by outsiders and insiders, and both intrusions and viruses, and illustrate the vulnerability of Virginia state and local government entities

Virginia IT Before September 11, 2001

Nature of Situation

Before September 11, 2001, Virginia's IT systems were already in a situation characterized by:

- A high level of inter-connectedness;
- Many viruses/worms and intrusion attempts;
- Internal intrusions/violations; and
- Potential vulnerability from fire, flood, and other natural disasters.

Virginia has taken a leadership position in web-based government and education, with many organizations using telecommunications and the Internet in conducting their business. This leadership role has also brought with it an increase in the probability of systems being breached. Projects such as COVA PIN, a multi-agency venture, have begun a trend of interconnecting systems. This inter-connectedness gives rise to opportunities for both external and internal security violations. Further complicating this, IT systems have to meet data privacy requirements.

The potential for e-mail, servers, and computer ports to act as mechanisms to deliver harmful code are compounded by the ability of employees to download potentially dangerous software from the Internet. Anti-virus software packages recognize more than 50,000 different intrusions. Some intrusion detection software recognizes more than 1,000 patterns of attack. According to the IT security research firm mi2g, the number of website defacements worldwide increased from 7,629 in 2000 to 30,388 in 2001.

Thus, the information security environment faced by Virginia state and local governments was already formidable before September 11.

Challenges for IT in Addressing Security

Given this environment, Virginia state, local government, and higher education IT departments faced a number of difficulties in addressing their information security problems before September 11 that continue today. These included:

- Assessing numerous business risks and business continuity;
- Establishing and maintaining an information security program;
- Managing the numerous software updates required to reduce vulnerabilities and enhance security;
- Ensuring compliance with security policies and procedures, which requires constant vigilance and resources;
- Dealing with the lack of standardization of procedures for persons to download and install software on their desktop machines;
- Following up on cases of e-mail and web browsing abuse;
- Maintaining adequate staffing, which is difficult within the state personnel system's constraints due to the market demand for qualified computer security personnel;
- Enforcing the state privacy strictures, which add additional security requirements and resource demands;
- Maintaining the capability to recover from disaster, which requires frequent plan updates and rehearsals; and
- Obtaining funding for security, which is often not the highest priority.

This long list of duties and difficulties further demonstrates that even before September 11 Virginia government IT security faced a formidable task.

After September 11, 2001

After September 11, the heightened awareness of terrorist threats has had a number of implications for organizations. These range from the need to restrict information potentially useful to terrorists, to dealing with the increased chance of severe attacks aimed at destroying or retarding the government's ability to respond or function.

In a special report in *Disaster Recovery Journal* (Oct. 1, 2001), speaking of businesses in and around the World Trade Center that were able to continue "business as usual" stated, "These companies relied on thorough, well-tested contingency plans and were able to switch their business operations to an alternative site … " In late 2001, 100 Virginia agencies were surveyed regarding their IT disaster recovery and security planning, with 81 responding. Of these, 71 reported having a disaster recovery plan and 10 said they had

no plan. Overall, 42 percent reported a disaster plan tested in 2001 and another 10 percent in 2000. Thirty percent reported never having tested their disaster plan or could not say when they had. With up-to-date, "well-tested" disaster plans being essential, the National Governors Association's (NGA) recent recommendation for "Contingency plans for government continuity and essential services when systems are down …" seems particularly relevant for Virginia.

To prepare for disaster recovery and to maintain business continuity, some Virginia state organizations have contracted for services that allow them to store network backup tapes of their systems off site. Then, in the event of either a physical or network disaster, their computerized information will not be completely destroyed.

Emergency Management

Whether IT departments are directly targeted or just suffer collateral damage, they must address the possibilities of physical, personnel, and electronic attacks – all of which can impact information security and the ability of IT systems to function. These include dealing with:

- Increased physical security;
- Local emergencies extending beyond state facilities;
- Critical infrastructure damage, particularly telecommunications failures;
- Massive destruction;
- Possible loss of people; and
- State emergency management needs.

These require re-planning, new and constant rehearsals, and additional coordination – placing increased strain on resources. A difficult job is now even more challenging.

Telecommunications are no longer a given in an emergency. On September 11, three million data lines running through Verizon's West Street facility in lower Manhattan were destroyed or damaged. According to *CIO Insight*, an early estimate by Computer Economics Inc. for restoring or replacing the IT and telecommunications infrastructure in and around the former World Trade Center and the Pentagon was $15.8 billion. Telecommunications require, according to the NGA, "A security assessment of all … networks including state owned and operated, leased, or contracted; … [and] a statewide interoperable communications system and emergency response call center." In general, state departments can benefit by sharing common tasks and providing mutual support.

Within the first 30 days of taking office, Governor Mark Warner issued Executive Order Seven, which established the Secure Virginia Initiative. In this executive order, the Governor directs state agencies "to prepare emergency response plans within the first 120 days and to address continuity of their operations and services, and the security of their customers and employees in the event of natural or man-made disasters or emergencies,

including terrorist attacks." The Warner administration has set in motion an evaluation process that begins with the Commonwealth's agencies and will next be handled by members of the Secure Virginia Panel who have been charged with developing a comprehensive emergency preparedness and response plan.

An older Executive Order Number Forty-one (99) promulgated the Commonwealth of Virginia Terrorism Consequence Management Plan dated April 1999. This plan provides for a coordinated government response to the effects of consequences of an actual terrorist act or the threat of such a violent act or actions in the Commonwealth. Each designated state department or agency shall: (1) Prepare and maintain the components of the plan for which it is responsible; (2) Conduct an ongoing training program and participate in exercises as needed in order to maintain an appropriate emergency response capability; (3) In time of emergency, implement emergency response actions as required and in coordination with the Virginia Emergency Operations Center; and (4) Assist with post-disaster restoration and recovery operations as required. In addition, the state legislature has proposed relevant laws.

The Virginia Department of Emergency Management's (VDEM) draft procedure in VDEM's *Virginia Terrorism Consequence Management Plan* attachment to Annex J– Infrastructure, Cyberterrorism deserves mention. Currently, this annex is pending approval from the Secretary of Technology. It discusses Emergency Management Actions for Cyberterrorism with topical headings including (1) Normal Operations, (2) Increased Readiness, (3) Response, and (4) Recovery.

Summary

Thus the danger and problems are real. The incident and emergency management contexts are constantly evolving at the local, state and federal levels. Next we will present steps an executive can take to begin addressing these problems in his or her organization.

Potential Executive and Manager Action Steps

As a Virginia governmental executive, what can you do to ensure your organization is prepared to deal with *"... a natural disaster, large-scale accident management and recovery, and of course, terrorist or military attack,"* (March 1, 2002, Press Release, *Secure Virginia Panel Convenes First Meeting*) as well as cyber attacks from the "usual" sources?

*This section directly addresses **you** as a Virginia governmental executive.*

This paper recommends three actions as a starting point in determining your organization's state of readiness:

- Use the following "Initial Questions" to determine how prepared your organization is to cope with an emergency. These questions are by no means exhaustive but should offer insight for establishing a more proactive response to an emergency or an unexpected event.

- Choose from the low budget actions offered to benefit your organization or stimulate additional actions.

- Implement a Virginia state standard on computer security, such as the standard included here.

Initial Questions

Below are several short sets of questions you as an executive or general manager might ask your IT manager, preferably accompanied by his/her IT security manager. (These latter might, of course, also find these questions useful.) The questions cover disaster recovery, protection against Internet attacks, personnel, security policies, software development and acquisition, hardware acquisition and maintenance, network security, and physical security.

> *"Given the wide range of threats we face, given their potential impact on public health and safety, the environment, our economy, and our citizens," said Governor Warner, "The question that I put before this panel today is: are we prepared?"*
>
> (March 1, 2002 Press Release, *Secure Virginia Panel Convenes First Meeting*)

Many experts recommend that a full risk assessment be performed as a basis for decisions and action. This initial set of questions does not constitute a full risk assessment. Use these questions to begin a dialogue with your IT department and its security personnel to help you establish an initial understanding of the situation in your organization. One result of this understanding should be a decision on when to invest in a full, formal risk assessment to fully inform the developing and implementing of a response strategy. Note that IT risk assessment is part of the normal audit requirements for every state agency.

Emergency Response and Disaster Recovery

You need to determine the level of preparedness at your agency. Here are some questions you should ask:

- Have we identified the systems essential for us to continue to perform our core mission?

- Are all our systems, including desktops, backed up daily?

- When was our IT emergency/disaster recovery plan last updated and last rehearsed or tested? Could I have a copy of the disaster recovery plan and the report on the last test or rehearsal?

Internet Attack/Inside Intruder Protection

You need to know what your agency has in place before trying to improve on it. Here are some questions that you should ask:

- Are we able to assist in investigation and prosecution of persons responsible for attacks, including evidence preservation?

- What firewall and anti-virus technology do we have installed and do they protect all our IT assets?

- How quickly do we know when we are being attacked?

- Do we have a Computer Incident/Emergency Response Team established? Does it have formal procedures and pre-assigned authority to act swiftly and decisively to defend the agency's infrastructure?

- Do we treat our computer logs as standard business records and retain them?

- Are procedures in place for timely notification to law enforcement?

Personnel

Properly trained staff is the first step in defending your agency's IT assets. This training encompasses all levels of expertise from technical staff to clerical staff to management. Some questions you should ask to determine the training level of your staff include:

- Is our Computer Incident Response Team trained to handle cyber attacks against the agency? Do they have IT-security-related certifications? What would be the result if we lost two or three of our most critical IT security personnel over the next four months?

- Are our system administrators properly trained in system administration security techniques?

- Are our system administrators trained in security? What background checks or other means of ensuring trustworthiness and reliability do we have for IT personnel and others with access to critical areas?

- Are our users and operators trained in computer security and "social engineering" attacks, such as phone calls asking for passwords? Do we use biometrics or physical tokens or devices anywhere for access?

- Do our users know whom to call in the event of a cyber emergency?

Security Policies

Your security policies must comply with existing state, local and federal laws and regulations. Here are some questions regarding your agency's preparation in the policy area:

- What privacy requirements must we meet? FOIA? HIPPA? FERPA?

- What do our IT-related security policies cover and when were they last updated?

- How do we enforce these policies? What violations did we have in the last six months, and what did we do?

- What awareness programs are in place to educate our staff on these policies?

Software Development and Acquisition

If your agency develops software or services, then you need to ensure that you are developing a safe product. Some questions you should ask include:

- In our own software development, do we give priority to security requirements and secure design and coding techniques?

- How extensive are our security requirements when acquiring software, and what priority do we give them?

- How would you characterize the level of security provided by our application software in use and under development?

Hardware and Network Acquisition and Maintenance

In most cases, the security of the agency's network is critical. Network-capable devices are often not designed/implemented with security in mind. Consequently, these insecure devices can threaten the security and integrity of your business operations. You should ask these questions:

- For our server and desktop acquisitions and maintenance, do we require vendors to report on the security of the devices or software they plan to sell to us?

- Do our system and network administrators have a minimum standard for security designed and implemented on all of our IT assets?

- When was the last time our network security was tested? By whom? And what was the disposition of the findings?

- Are all our wireless networks encrypted, and how secure is this encryption?

- Do we allow modem connections that could permit security breaches? Do we have caller-id enabled for our modem pool?

Physical Security

One of the most basic audit requirements involves the physical security of IT assets. Some questions you should ask in this area:

- Do we have around-the-clock, seven-days-a-week physical security for our computing and telecommunications facilities, with human and electronic surveillance?

- What could a physical attack such as a truck bomb do to us?
- How easy is it to gain access to desktops with access to our critical systems?

Coordination

One of the most critical aspects of incident response is the containment of the attack. Sometimes, this requires communication with other state agencies. You need to determine if your agency has access to cyber security information channels. Along the way you should identify all the vendors and services used to aid in IT security. You might later concern yourself with how well these and other internal and external elements – particularly state and local public safety agencies – work together to provide protection, damage confinement, and recovery.

Conclusion

While the initial answers you receive to some of these questions may very well disturb you, use them to begin a dialogue with your IT department and its security personnel leading to an improvement program. These initial questions offer a starting point. For more in-depth analysis, it would be prudent to engage your IT manager and security officer or engineer and have them further explore these areas by answering the self-assessment questions found in the appendix. If for specific areas of concern priorities need to be changed to include security actions (e.g. network security), request that the lead manager or engineer create a plan of action to quickly take positive steps to increase security.

Specific Low Budget First Steps

This section provides a few specific suggestions regarding computer security that can be taken without requiring special funds. They will take some time and effort, but this should not be excessive. These steps include use of free software to check the settings of computers for security problems; review of susceptibility to the most common problems; and education and certification of personnel.

CIS Benchmarks

The Center for Internet Security offers free software to check on the setting of several operating systems for potential security problems. They also offer benchmark documents that contain the steps needed to increase the security of a machine. These benchmarks were developed with the involvement of a number of commercial, government and educational sources and have become de facto standards in the Internet community. While the software only checks one machine at a time, its score (10 is best) provides a way for non-technical people to evaluate their organization's machines' settings. (See www.cisecurity.org)

"Top 20" Internet Threats List

The SANS (System Administration, Networking and Security) Institute, in coordination with the FBI and with substantial industry involvement, developed first a "Top 10" and more recently a "Top 20" list of vulnerabilities most commonly exploited by attackers. Generally these involve settings or practices, or use of particular software or software versions. (See www.sans.org/top20.htm)

Your IT organization should review its systems using the points relevant to each system. These "Top 20" vulnerabilities are regularly updated.

Seminars

Computer security seminars are offered by a number of organizations. These vary in price and intended audience. The Commonwealth Information Security Center at James Madison University regularly offers inexpensive seminars for managers around the state. Virginia Tech has hosted a number of security seminars for free to state IT staff. (See www.cisc.jmu.edu and http://security.vt.edu)

Personnel Certification

Aiming for and achieving security-related certifications can motivate security personnel and help provide evidence of minimum competence on the part of your security staff. Among these certifications are a variety of technically oriented ones offered by the SANS Institute and the more general CISSP and others from the $(ISC)^2$ Institute. Relevant certifications are also available from such vendors as Microsoft, Oracle, and Cisco. (See www.giac.org and www.isc2.org)

Internal Audit

You might consider conducting an internal audit. If your organization has an internal audit organization, this is an obvious source for independent auditors. Nevertheless, a team of auditors with all the different kinds of expertise may be difficult to assemble from persons independent from those being audited.

Conclusion

These are a few low budget actions. Your IT department should be able to suggest more. Encourage them to address security despite any budget constraints. A more comprehensive – but not necessarily inexpensive – set of steps is included in the standard discussed next.

A Standard

In 2001, the Department of Technology Planning released SEC2001-01.1, a detailed information technology security standard that was developed for use by all state agencies within the Commonwealth of Virginia. This standard is a road map that agencies should

use to establish an effective and strong defense against unauthorized intrusions to networks. The establishment of an Information Systems Security Officer (ISSO) is listed as a must for agencies. The ISSO is responsible for coordinating the agency's information technology security efforts through the establishment of a security architecture. The architecture consists of 13 components, which are shown in the box on the right.

By establishing an ISSO and implementing this security standard, an agency head will fulfill his or her responsibility to exercise due diligence in the protection of the agency's network. Review and implementation of the security standard is a positive first step toward effectively managing the vital network security for an agency. (See www.cim.vipnet.org/pubs/dtp-pubs.htm#Standards)

Standard SEC2001-01.1 Areas

Business Analysis and Risk Assessment
Security Awareness
Technical Training
Authentication, Authorization, and Encryption
Data Security
Systems Interoperability Security
Physical Security
Personnel Security
Threat Detection
Security Tool Kit
Incident Handling
Monitoring and Controlling System Activities
Technical Communications

Conclusion

The Virginia governmental information security environment could be dramatically impacted by an act of terrorism or other disastrous situations. Virginia needs to be prepared for these threats. Improving each organization's IT security practices can greatly reduce the risks involved.

This paper was written to help Virginia governmental or educational executives address the preparedness concerns cited by the Governor, and to help them determine whether existing internal procedures for IT readiness actually fulfill their responsibility to perform "due diligence" for the citizens of Virginia in securing their computers and network(s).

Executives may find their organizations to be in excellent shape, but unfortunately may also find them in a less than acceptable and highly vulnerable condition. The recommendations in this paper can help strengthen organizations' IT security. Many opportunities exist to make improvements within current budgets.

Executives should begin a dialogue with their IT and IT security managers to start the process. Use the questions provided here to begin discussions and work toward improvement. Aim to sleep well at night and avoid finding a department saddled with excessive recovery expenses, unable to deliver services, or making media headlines.

Appendix: Initial Self-Assessment

Emergency Response and Disaster Recovery

- Have we identified the systems essential for us to continue to perform our core mission?
- Are all our systems, including desktops, backed up daily?
- When was our IT emergency/disaster recovery plan last updated and last rehearsed or tested?
- Are our recovery and continuing operations instructions written as simple, clear, complete sets of steps that upset, fatigued persons could follow correctly?
- Did the testing include full simulation of loss of computer equipment and telecommunications services, plus the possibility of loss of some personnel and the execution of every alternative contingency and recovery step?
- Are tests of the plan frequent and the results satisfactory?
- Do I have a copy of the disaster recovery plan and the report on the last test or rehearsal?
- What will be the interruptions before essential and other services are up and available from our offsite facility?
- What will be our backup once we are operating from our offsite facility?

Internet Attack/Inside Intruder Protection

- Are we ready to assist in investigation and prosecution of attackers?
- What firewall protection do we have installed today?
- Does the protection extend to all IT assets and is the protection in-depth?
- How do we know when a new type of attack appears?
- How do we know when we are being attacked?
- Are the logs and records we keep sufficient to:
    - Identify intruders and their exact methods?
    - Assist in investigation and prosecution?
- Do we treat our computer logs as standard business records? Are they integrated into our business record retention procedures?
- Do all our platforms, including desktops, have virus protection and (personal) firewalls that are automatically kept up-to-date?
- Do we have proper network router configurations to offer up-to-date protection?
- Should a reputable third party perform a system penetration test?
- Do we have a Computer Incident/Emergency Response Team established?
- Does it have formal procedures for reporting and responding to incidents and have those procedures been tested?
- Does the team have the pre-assigned authority to act swiftly and decisively to defend the agency's infrastructure?
- Do we manage intrusion detection in the manner we should?
- Do we have daily review and follow-up actions taken after reported intrusion incidents?
- Am I given a copy of this report?

Personnel

- Do we have experienced, expert personnel doing security?
- Do they have IT security-related certifications?
- Is our Computer Incident Response Team trained to handle cyber attacks?
- What would be the result if we lost two or three of our most critical IT security personnel over the next four months?
- Are our system administrators properly trained in system administration techniques?
- Are our system administrators trained in security?
- What background checks or other means of ensuring trustworthiness and reliability do we have for IT personnel and others with access to critical areas?
- Are our users and operators trained in computer security and "social engineering" attacks such as phone calls asking for passwords?
- Do users of any of our systems have to use biometrics or physical tokens or devices as well as passwords in order to access them?
- Do our users know whom to call in the event of a cyber emergency?

Security Policies

- What privacy requirements must we meet? FOIA? HIPPA? FERPA?
- What do our IT-related security policies cover?
- When were they last updated?
- What awareness programs are in place to educate our staff on these policies?
- How do we enforce these policies?
- What violations did we have in the last six months, and what did we do?
- How do we know if these were all the violations?
- What policies do we have to ensure and maintain security of our network(s) including our LANS?

Software Development and Acquisition

- In our own software development, do we give priority to security requirements and secure design and coding techniques?
- How extensive are our security requirements when acquiring software, and what priority do we give them?
- How would you characterize the level of security provided by our application software in use and under development?

Hardware and Network Acquisition and Maintenance

- For our server and desktop acquisitions and maintenance, do we require vendors to report on the security of the devices or software they plan to sell to us? On security implications of settings?
- How do we establish and maintain desktop security including desktop firewalls?
- Do our system and network administrators have at least a minimal security standard designed and implemented on all of our IT assets?
- When was the last time our network security was tested?
- Who tested the network?
- What was the disposition of the findings?
- Do we maintain an accurate and up-to-date inventory of our network IP addresses?
- Are all our wireless networks encrypted?

- How secure is this encryption?
- Do we allow modem connections that could permit security breaches? Do we have caller-ID enabled for our modem pool?

Physical Security

- Do we have around-the-clock, seven-days-a-week physical security for our computing and telecommunications facilities with human and electronics surveillance?
- What could a physical attack, such as a truck bomb, do to us?
- How easy is it to gain access to desktops with access to our critical systems?

Coordination

- Do we have a list of all the vendors and services we use for IT security?
- Do we know how vendors and our state and local public safety agencies work together to provide protection, damage confinement and recovery?
- Have we developed points of contact with law enforcement agencies (Virginia State Police, FBI, Office of the Attorney General) whom we would notify and assist in investigation and prosecution of attackers?

Commonwealth Information Security Center Technical Report CISC-TR-2002-002

Commonwealth Information Security Center
MSC 4103
James Madison University
Harrisonburg, Virginia 22807